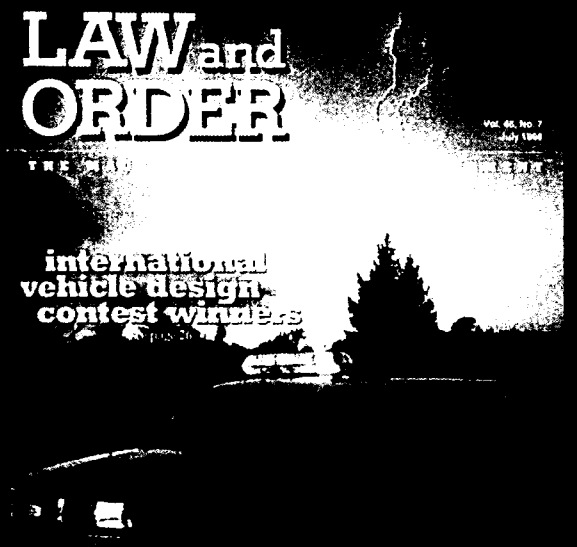
Operational Planning

Taking the Adversary's Perspective



Focus Topic: Mobile Patrol

special report I: interrogations

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 83335A
20 June 2019

MUCKROCK NEWS
DEPT MR 22858
411A HIGHLAND AVE
SOMERVILLE MA 02144-2516

Dear Mr. Best:

This responds to your Freedom of Information Act (FOIA) request, which was received by this office on 23 September 2016, for "'Maintaining Operational Security: Minimizing the Risk of Law Enforcement Mission Failure' and its companion piece 'Operational Planning: Taking the Adversary's perspective', which were reprinted from Law and Order Magazine and offered through the Interagency OPSEC Support Staff in the information Assurance Directorate." As previously provided, your request has been assigned Case Number 83335. There are no assessable fees for this request. Because there are no assessable fees for this request, we have not addressed your request for a fee waiver.

Your request has been processed under the provisions of the FOIA. Enclosed is the material you requested. If you need further assistance or would like to discuss any aspect of your request, please do not hesitate to contact me at foialo@nsa.gov or you may call (301)688-6527.

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877/684-6448
(Fax) 202/741-5769

Sincerely,

Michael Hudson
for

JOHN R. CHAPMAN
Chief
FOIA/PA Office

Encl:
a/s

The Interagency OPSEC Support Staff

Our **Vision** is secure and effective operations for all National Security mission activities.

Our **Mission** is to promote and maintain OPSEC principles worldwide by assisting our customers in establishing OPSEC programs, providing OPSEC training, and conducting OPSEC surveys.

Our **Goal** is to be recognized as the leader and preferred provider of value-added OPSEC products and services.

INTERAGENCY OPSEC SUPPORT STAFF

OPERATIONAL PLANNING

Taking the Adversary's Perspective

By

John E. Glorioso Sr. and Robert B. Ritter

Mr. Glorioso is currently serving as an OPSEC Program Developer with the Interagency OPSEC Support Staff (IOSS). His primary responsibility is to develop OPSEC organizational and training programs for various U.S. government executive departments and agencies, with a primary focus on working with the law enforcement and intelligence communities. Prior to his employment with IOSS, Mr. Glorioso served 25 years with the Maryland State Police, retiring in 1986 as a First Lieutenant. He holds an MS degree in Human Resource Development and an MA degree in Psychology. Mr. Glorioso has published several articles; his latest, "Maintaining Operational Security," was published in *LAW and ORDER* magazine in October 1996.

Mr. Ritter, currently the Deputy Director, has been assigned to the IOSS since January 1992. A long-time federal security officer, Mr. Ritter has had the opportunity to utilize OPSEC throughout his career in a wide variety of situations. In his capacity as a Senior OPSEC Officer, he has provided training and guidance to a large number and mix of local and federal law enforcement organizations, as well as military and civilian departments and agencies. Mr. Ritter holds a B.S. degree in Police Administration, and co-authored "Maintaining Operational Security" with Mr. Glorioso.

Reprinted with permission from the July 1998 issue of *LAW and ORDER* magazine

The Monograph Series

This document is published and distributed as part of the Interagency OPSEC Support Staff Monograph Series. Documents in this series are intended to provide resource materials to assist the U.S. government executive departments and agencies and their supporting contractors in establishing and maintaining their OPSEC programs.

Manuscripts may be submitted to the IOSS for inclusion in the Monograph Series. All manuscripts will be acknowledged on receipt; a decision to accept or reject will be made as quickly as possible. Responsibility for U.S. government clearance of articles (when required) and clearance for copyrighted material lies with the author. Publication of the manuscripts does not imply endorsement by the IOSS or any other U.S government department or agency, nor does it obligate the U.S. government to sole source procurement of goods or services.

The IOSS does not provide an honorarium for authors. Unless otherwise requested by the author, the IOSS reserves the right to use all published material as part of any or all of the IOSS activities in support of the IOSS mission.

The manuscripts may be classified or unclassified. However, in order to reach the widest possible audience, it is preferred that they be unclassified. A brief biographical sketch of all authors should be provided with all submissions. This should include current position, government department, company, or military assignment, and if military, rank and branch of service.

Please submit any manuscripts, comments, or suggestions concerning this publication to the IOSS at the address listed below. Please call for any additional information concerning the OPSEC Monograph Series, this publication, or handling instructions for any classified materials.

Interagency OPSEC Support Staff
6411 Ivy Lane
Suite 400
ATTN: Publications Department
Greenbelt, MD 20770-1405

Phone: (301) 982-0323/2313
FAX: (301) 982-2913

OPERATIONAL PLANNING

Taking the Adversary's Perspective

"The best way to catch a criminal
is to think like a criminal."

Those who have spent even a few years in law enforcement have heard this adage in one form or another. The saying refers to law enforcement officers who can separate themselves from viewing a situation from only one perspective (the good guys) and can include the view of their adversary, and thus have a better chance of apprehending the criminal. In reviewing the performance of officers who seem to have this ability and who have applied their "street-craft" effectively, there seems to be some truth in the maxim.

On the street, the skill to view a situation from the criminal's viewpoint can be very productive. We need to take this idea and apply it to the planning and execution of our operations.

By viewing our operation from the eyes of the adversary, we can determine what information criminals may need from us in order to be successful. In the criminal mind, success means they win — we lose.

One way of employing this adversary perspective is to use a process utilized extensively in operations security (OPSEC). This process is referred to as the "adversary strategy."

When applied during the OPSEC process, the adversary strategy can provide valuable information that will aid in both the planning and execution of police operations. It does this by providing those planning the operation the opportunity to view the mission from the viewpoint of the criminal. This perspective permits planners to determine what information criminals will need from law enforcement to be successful.

For those new to the operations security concept, OPSEC was described in an earlier edition of *Law and Order* (October 1996) as a method of taking a holistic view of our mission from the standpoint of the adversary. Through those eyes, we view our operation to determine what information is crucial for our success and where the information may be lost. Once identified, we conduct a risk assessment and apply countermeasures to those actions that have the potential for exploitation by the criminal. In short, OPSEC attempts to deny potential adversaries the ability to determine our intentions and capabilities by identifying and protecting actions associated with our operations.

The OPSEC process consists of five steps and can be applied to any law enforcement operation, especially during the planning stage:

- Identifying Critical Information,
- Conducting a Threat Analysis,
- Performing a Vulnerability Analysis,
- Assessing Risk, and
- Applying Countermeasures.

The OPSEC process has been described by organizations that have applied the concept to their missions as a flexible and effective procedure that increases the probability of a successful conclusion. For police, the process provides a formal structure to study the criminal to determine if the adversary has the capability to collect, analyze, and use information against police efforts to gather sufficient evidence against the criminal element to successfully conclude their investigation.

The Adversary Strategy

The application of the adversary strategy pertains to the first two steps of the OPSEC process. By using OPSEC to study the criminal's intelligence gathering capability and applying law enforcement's "street-craft," planners of an investigation can look at their operation through the eyes of the adversary. This enables them to postulate the objective of the criminal and predict the different courses of action the criminal can take to foil law enforcement's efforts to be successful.

By determining the adversary's action(s), the planner will discover the information needed by the criminal to block law enforcement's effort to apprehend and prosecute the criminal. Once that critical information is identified, police can take measures to protect this information from being lost.

To better explain the concept of the adversary strategy, let's apply it to a possible law enforcement operation. Suppose members of a strike force have been directed to solve a series of high profile crimes occurring throughout the state. The strike force consists of criminal investigators from three county police departments, two city departments, and the state police. Through solid investigative techniques, the strike force has located a key witness to a major crime that will link the criminal enterprise under investigation to the offense. One investigator has successfully persuaded the witness to provide the information that will lead to the arrest of the remaining gang members.

A team has been assigned to protect and move the witness from a safe-house in the northeastern part of the state to the state capital, approximately 200 miles away. Realizing the importance of the person supplying the information, we want to exercise every possible precaution to assure the movement will be successful. We will apply the adversary strategy to our assignment.

Our goal is to retain the element of surprise when moving the informant. To do this, we must identify the information critical to our operation and prevent anyone not associated with the move from obtaining the facts. The team understands that the adversary strategy permits us to determine the possible courses of action the criminal gang may take to prevent us from reaching our objective. By identifying these projected choices of action, we can ascertain what information the gang needs from us to meet their goal.

Adversary strategy uses a form of a chart or decision tree to reflect the correlation of pieces of data regarding the operation. By placing information in a distinct area, the process permits us to focus on the crucial steps requiring attention. It will also provide a pictorial account of our efforts as we develop our plan of operation.

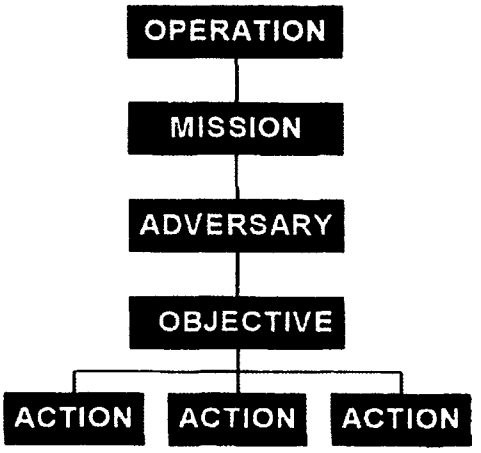


Figure 1

When completed, the structure will appear as in Figure 1.

As Figure 1 indicates, the first two boxes refer to the organization/unit performing the mission. In our case, the organization is the Strike Force; its mission is to protect and move the confidential informant. Therefore, the decision tree takes form.

The next two boxes refer to the adversary and their objective. In our case, it would be the criminal gang; and their goal is to prevent the witness from

talking. The chart then appears as in Figure 2.

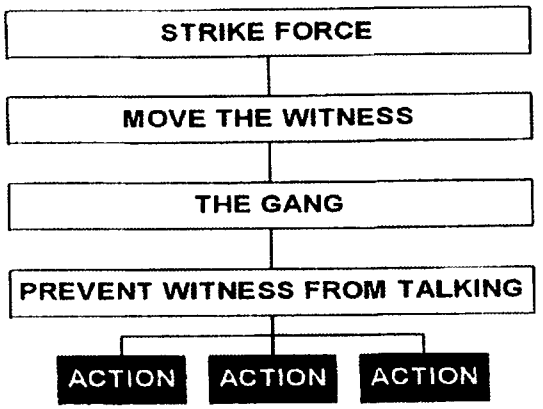


Figure 2

The next step is to predict the possible actions the gang could take in reaching their objective. This is where the process often differs from the normal preparation planners take. The concept forces us to look at the operation from the opponent's viewpoint and answer the question, "If I were the criminal, what would I do to prevent police from reaching their objective?"

Very simple, very basic, but extremely important. It is essential if the team moving the witness is to be successful.

A planner would sit down with key people in the overall operation and use the collective intelligence of the group. By answering the above question, the planning team would realize that the adversary has several options: kill the witness at the safehouse; kill the witness en route to the state capital; or kill the witness at the courthouse.

Our chart then looks like Figure 3.

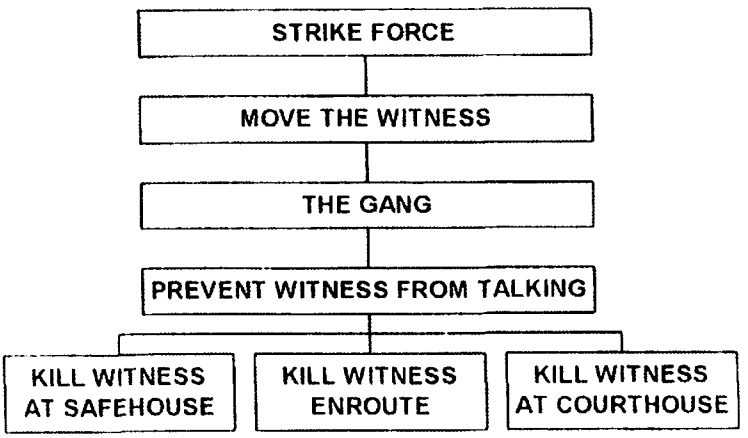


Figure 3

The next step is to determine what information the "gang" needs from law enforcement to be effective in preventing the witness from talking. In OPSEC terms, what is the critical information law enforcement must protect from the criminals in order to bring the mission to a successful conclusion?

To accomplish this task we simply list the possible course(s) of action horizontally and place the information they would need beneath the specific action. Remember, during this step we need to think like the criminal to determine the information they need from the police to eliminate our problem.

Thus, our adversary strategy would look like Figure 4.

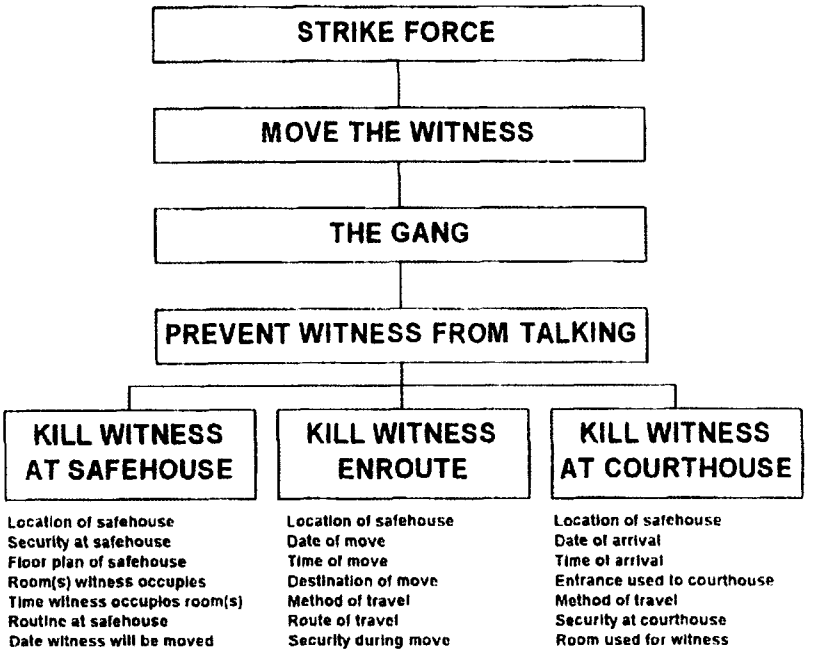


Figure 4

The team must review the chart and combine the pieces of information into one composite list. This list will be the critical information that must be protected from the gang during the movement phase.

Next, the planning team will analyze the threat to determine if the gang has the capability to collect police intelligence. The collection may be electronic (scanners, etc.), human (individuals sympathetic to the gang, insiders, etc.), photographic (cam recorders, still photos, etc.), or reading the trash (trash intelligence, "garbology," etc.).

Completing the threat analysis, planners would search for possible vulnerabilities connected with the operation. For example, the planning team

would answer the questions re whether or not they are

- Projecting intentions through established patterns of behavior associated with past missions,
- Conducting shift changes at the safehouse on a routine basis,
- Delivering food to the safehouse on a routine basis,
- Using local restaurant/fast food delivery (pizza, Chinese, etc.),
- Transporting witness to and from task force office on routine basis,
- Communicating our plans over unsecured police radios,
- Parking traditional unmarked police vehicles in front of the safehouse.

A risk assessment must be conducted. The team would link any vulnerabilities/indicators associated with the mission to the ability of the adversary (criminal gang) to collect and use the exploitable information. If it is determined that any of the vulnerabilities/indicators have a high risk, the planners would apply countermeasures to negate or reduce the discovered weaknesses.

For example, if changing security at the safehouse occurs at the same times each day, the countermeasure may be to simply develop an alternating schedule. The same process would be used if it was found that the same detectives always transport the witness to and from police headquarters or the field office being used for interviewing in the same vehicle, following the same route.

More Than One Adversary

There may be more than one adversary involved in an operation, but the adversary strategy can still be used. The process can be used regardless of the number of adversaries involved.

For example, in the previous exercise there may be one or more rival gangs interested in interfering with the movement of the informant. The adversary strategy would look like Figure 5 [found on the next page].

Although most operations planned by police managers, criminal investigators, and/or street officers are successful, there is a need to focus on those operations that have not met with success. Sometimes the criminal was just plain lucky and avoided arrest. Perhaps those other times, when a mission was not successful, police may have projected their intentions, failed to practice good communications security, or the critical information was inadvertently released by an associate or team member. That is why it is important to take a fresh look at how missions are planned.

Figure 5

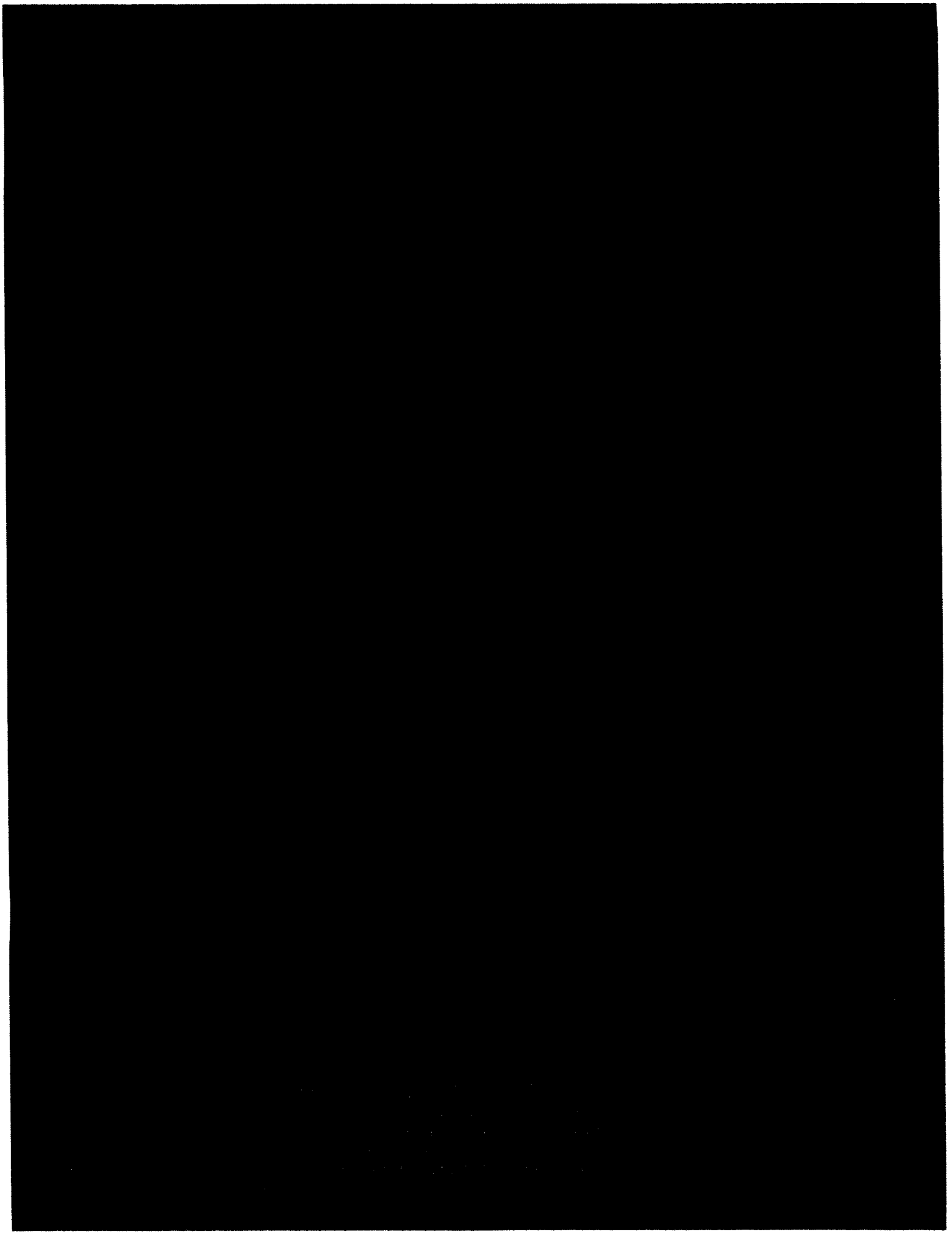
The Value of an Adversary Strategy

The value of using the adversary strategy is that it provides planners with a method of taking a holistic view of the mission being planned. A method that is simple, yet systematic, in the way it is conducted. By studying the criminal's capability of collecting information against law enforcement, it forces the planner to take protective measures.

When the strategy is used correctly, the planner will postulate the criminal's possible course(s) of action, identify the information the criminal needs to avoid arrest and place those contingencies necessary to protect information loss in order to meet the goals of the operation.

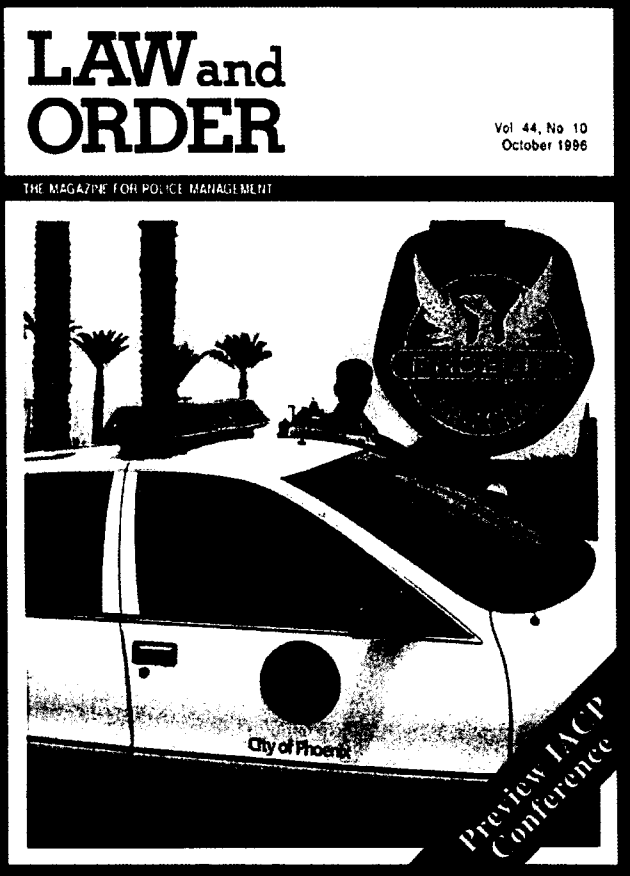
The adversary strategy encourages team involvement in an effort to utilize the collective intelligence of personnel and to incorporate various perspectives of how the criminal may react in a given situation. When used during planning, the adversary strategy provides a solid foundation for the operations security (OPSEC) process.

The benefits and incentives for incorporating OPSEC into the planning phase may vary from increased arrest, case closures, and cost-effective operations. However, the main reason to use the methodology is for the safety of the law enforcement personnel involved in the operation.



Maintaining Operational Security

Minimizing the Risk of Law Enforcement Mission Failure



The Interagency OPSEC Support Staff

Our **Vision** is secure and effective operations for all National Security mission activities.

Our **Mission** is to promote and maintain OPSEC principles worldwide by assisting our customers in establishing OPSEC programs, providing OPSEC training, and conducting OPSEC surveys.

Our **Goal** is to be recognized as the leader and preferred provider of value-added OPSEC products and services.

INTERAGENCY OPSEC SUPPORT STAFF

MAINTAINING OPERATIONAL SECURITY

Minimizing the Risk of Law Enforcement Mission Failure

By

John E. Glorioso Sr. and Robert B. Ritter

Mr. Glorioso is currently serving as an OPSEC Program Developer with the Interagency OPSEC Support Staff (IOSS). His primary responsibility is to develop OPSEC organizational and training programs for various U.S. government executive departments and agencies, with a primary focus on working with the law enforcement and intelligence communities. Prior to his employment with IOSS, Mr. Glorioso served 25 years with the Maryland State Police, retiring in 1986 as a First Lieutenant. He holds an M.S. degree in Human Resource Development and an M.A. degree in Psychology. Mr. Glorioso has published several articles; his latest, "Operational Planning," was published in LAW and ORDER magazine in July 1998.

Mr. Ritter, currently the Deputy Director, has been assigned to the IOSS since January 1992. A long-time federal security officer, Mr. Ritter has had the opportunity to utilize OPSEC throughout his career in a wide variety of situations. In his capacity as a Senior OPSEC Officer, he has provided training and guidance to a large number and mix of local and federal law enforcement organizations, as well as military and civilian departments and agencies. Mr. Ritter holds a B.S. degree in Police Administration, and co-authored "Operational Planning" with Mr. Glorioso.

Reprinted with permission from the October 1996 issue of *LAW and ORDER* magazine.

The Monograph Series

This document is published and distributed as part of the Interagency OPSEC Support Staff Monograph Series. Documents in this series are intended to provide resource materials to assist the U.S. government executive departments and agencies and their supporting contractors in establishing and maintaining their OPSEC programs.

Manuscripts may be submitted to the IOSS for inclusion in the Monograph Series. All manuscripts will be acknowledged on receipt; a decision to accept or reject will be made as quickly as possible. Responsibility for U.S. government clearance of articles (when required) and clearance for copyrighted material lies with the author. Publication of the manuscripts does not imply endorsement by the IOSS or any other U.S government department or agency, nor does it obligate the U.S. government to sole-source procurement of goods or services.

The IOSS does not provide an honorarium for authors. Unless otherwise requested by the author, the IOSS reserves the right to use all published material as part of any or all of the IOSS activities in support of the IOSS mission.

The manuscripts may be classified or unclassified; however, in order to reach the widest possible audience, it is preferred that they be unclassified. A brief biographical sketch of all authors should be provided with all submissions. This should include current position, government department, company, or military assignment, and if military, rank and branch of service.

Please submit any manuscripts, comments, or suggestions concerning this publication to the IOSS at the address listed below. Please call for any additional information concerning the OPSEC Monograph Series, this publication, or handling instructions for any classified materials.

Interagency OPSEC Support Staff
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405
Phone: (443) 479-4677
FAX: (443) 479-4700

Maintaining Operational Security

Minimizing the Risk of Law Enforcement Mission Failure

As the early morning sun appeared over the horizon, the sergeant in charge of the narcotic unit's raiding team contacted the on-site SWAT team commander to coordinate final plans to execute a search and seizure warrant. When the order was given, the entry team hit the house with lightening speed. Gaining access to the house, the SWAT team began a systematic search. The narcotic unit followed and also looked for the perpetrator and the drugs said to be in the house. After a thorough search, nothing was found—no suspect and no drugs.

At the debriefing, the officers involved openly questioned what went wrong. Was there a snitch? Were the wrong leads followed? Or were they fooled by the criminals?

In reviewing the case, one thing was certain: the information critical to the success of the operation was lost. The loss could have been in response to one of the questions posed by the officers associated with the case. Or, and these are more likely the reasons for the failure, the critical information could have been inadvertently lost by not following proper communications security, or the information could possibly have leaked out by broadcasting the intentions of the upcoming raid through predictable patterns of behavior.

By analyzing the operation in a systematic manner, it may be determined that the information critical to the success was the date, time, and location of the raid. Additional essential data could be that a particular person was targeted, a search of his residence would take place, and the suspect would be arrested based on probable cause.

What the planners failed to consider was that the adversary might have been monitoring police channels with the aid of a scanner or collecting information by frequenting various establishments (restaurants, bars, etc.) where officers gather and talk. The suspect could have used the information gained by his communications intelligence to block law enforcement's efforts.

Another possible answer could be that indicators associated with the intentions of the police mission were detected by the suspect. Normal activities associated with police operations could point to the intention(s) of the police. Some possible indicators could include the surveillance of the residence by undercover vehicles (which might be known to the criminal community), inquires made by undercover officers about the suspects, or the routine, normal ways we do things that might alert others to our intentions.

After observing these patterns of performance and activity, the suspect might have determined that he was the potential target. Armed with this knowledge, he was able to counter the actions of the police.

Progressing through the analysis, it may be discovered that, as a result of not ensuring that the police communications were secure, valuable information was broadcast over the airwaves, susceptible to interception by anyone with an easily obtained scanner. Any, or all, of these concerns could have been present in our scenario.

If the police planners had known the criminals were being provided the means to thwart their goals, they could have changed their methods and procedures (i.e., taken countermeasures). Systematically reviewing the operation by focusing on determining critical information, identifying the adversaries, ascertaining how the adversary could collect the information (watching or listening to police, etc.), and determining countermeasures is part of a process known as Operations Security (OPSEC).

The Origin of OPSEC

OPSEC originated during the Vietnam War to ensure the element of surprise in favor of U.S. forces. During the early days of the war, the U.S. military was faced with a dilemma. Many of their operations did not succeed as planned. Searching for a way to locate and fix the discrepancies, a team was assigned to survey several missions to provide answers. Their activities included interviewing key operational people, following the flow of information, observing part or all of a mission, and then offering recommendations on how to improve the operation.

An example of such a survey involved the B-52 bombing missions over Vietnam. Military leaders believed that elements of critical information were being leaked prior to the flights. The enemy used this knowledge to thwart the Allied efforts, fading into the surrounding countryside just prior to the air strikes.

The command staff requested a survey of one of these operations to determine the cause of the problem. A spy or snitch was ruled out when it was discovered the information was inadvertently "leaked" by following routine, predictable patterns of behavior. The one pattern that proved especially vital was the filing of standard flight plans for the B-52s, including the arrival and departure times over the target area and the flight paths the aircraft would be taking.

This process had been followed for some 20 years. Because it was so natural and ordinary, no one gave it much thought—that is, until the OPSEC team happened upon it. They found that Hanoi was one of the recipients of the flight plan information. A countermeasure followed swiftly (a generic flight plan, with no specific times or routes, was filed). Air strike efficiency increased greatly.

The Department of Defense (DOD) continued to use OPSEC after the war, although at a reduced pace. In 1988, President Reagan signed a directive that formalized the use of OPSEC throughout the U.S. government where national security issues were involved. This directive assigned a top-level manager the responsibility to serve as Executive Agent for the program and established the Interagency OPSEC Support Staff (IOSS) to provide training and program development guidance and assistance throughout the federal government.

However, the benefits associated with OPSEC are not limited to federal agencies or departments. OPSEC can be used by any organization, government or private, desiring to protect sensitive or critical information. While much of the emphasis has been placed on the military and federal law enforcement, OPSEC is just as appropriate to state and local law enforcement agencies. Conscientious use of OPSEC in planning and executing police operations is a proven means of increasing efficiency and saving resources (time, money; and perhaps, lives).

OPSEC Defined

Operations Security is a process to deny potential adversary information concerning the capabilities and intentions of an operation by identifying, controlling, and protecting indicators associated with the planning and execution of a mission. The OPSEC process consists of five steps that can be reviewed prior to or during the planning of a law enforcement operation:

- Identifying Critical Information,
- Conducting a Threat Analysis,
- Performing a Vulnerability Analysis,
- Assessing Risks, and
- Applying Countermeasures.

The reason these five steps are not numbered is that the process does not have to be followed in a linear fashion. OPSEC is fluid, allowing the manager of a case or mission to use the process in the manner that fits the particular situation. One federal law enforcement agency often begins with identifying the adversary or adversaries they may face in their operation, then postulating what information this person or persons might need to block the operation. The remaining steps are then addressed.

OPSEC allows a manager to ensure success of an operation by systematically reviewing it prior to its beginning. What makes OPSEC different from other management procedures is that OPSEC focuses on the threat—those individuals who want to block an operation or make it fail in order for them (the bad guys) to be successful.

For law enforcement, effectiveness means

- no loss of life or injuries to law enforcement personnel,
- arrest of perpetrators,
- convictions in court,
- collection of evidence, and
- protection of society.

OPSEC allows law enforcement to look at an operation through the eyes of the adversary to determine how and where information critical to the success of an operation may be lost. OPSEC permits police managers to realize the adversary needs information from police to make their (the

criminal) mission successful. The criminal wants to know law enforcement's intentions, their contacts, how police communicate, and various operational procedures used by police in conducting their operations.

THE FIVE-STEP OPSEC PROCESS

Critical Information

The first step in the OPSEC process is to establish the critical information. This normally includes the facts about the operation, intentions, and capabilities that need to be kept secret. Identifying the critical information associated with a case can be approached from two perspectives.

The approach endorsed by a majority of those using OPSEC is to view critical information from the adversary's perspective. That is, what does the adversary need to make his operation successful? Police management must ask, "If I were a criminal, what data would I need to avoid arrest?" If the adversary is a drug dealer, and his objective is to avoid arrest, the critical information needing protection might be that there is actually a plan to arrest the person, the identity of the informant who may be providing the police with information, the identity of an undercover officer, and the date and time of the planned arrest.

The other method is to view information believed to be essential for a favorable outcome to a police operation as "data requiring protection," from the perspective of the police planner. Such information might include the names of undercover investigators, informants, date and time of an operation, the target of an investigation, and any other piece of information that needs protection. In this approach, we are interested in protecting the critical information the planner believes is important for success from his/her viewpoint, not what the adversary needs to be successful.

In one raid, a book owned by a criminal was found to contain pieces of information concerning law enforcement agencies. The criminal separated federal, state, and local departments into sections and further subdivided those agencies. Included in his data bank were tag numbers and makes of undercover police vehicles, plus the names, phone numbers, and, in some cases, home addresses of undercover officers.

Threat Analysis

The next step of the process directs attention toward two separate, independent factors of the threat. One aspect addresses the person or persons who might be trying to get the information; the other element is the method used in collecting the information.

An adversary is anyone who opposes, or acts against, law enforcement's interests. This may be anyone who requires the knowledge concerning what is being done and who may have an impact on the mission.

The adversary might be the actual target, the suspect in a robbery case, a person for whom warrants are going to be served, or any other person(s) who is the focal point of the investigation. This type of person can be referred to as the "active" adversary.

An adversary could also be someone not directly involved in the specific crime under investigation, but one who supplies information to the suspect regarding an activity. This individual can be referred to as a "passive" adversary. In one operation, it was observed by police that every time a drug interdiction vessel left port, an individual sitting on the pier fishing would get up and make a phone call. When interviewed, the fisherman reported that he was given money to call a specific phone number every time the particular vessel left port.

A different type of adversary might be someone "on our side" who inadvertently provides information to the criminal. This could be something as innocent as being overheard at a restaurant, to having plans being given to the media through a public information officer.

In one murder investigation, a police spokesperson provided an update regarding the progress of the case to the news media. The officer informed the media of the department's plan to maintain a surveillance of the suspect's residence. Needless to say, if the suspect read the local newspaper, he probably wouldn't return to his residence.

The second element in this step is the method used to collect intelligence against a police operation. Collection methods vary depending on the level of sophistication of the criminal. These various modes of gathering intelligence run the gamut, from using electronic equipment to searching through someone's trash.

Some of these methods are listed as follows:

- Communications. The use of electronic devices to obtain information on police operations and personnel. Scanners can monitor police radio networks or cellular telephone conversations.
- Imagery. The use of still or video cameras to obtain visual representations of police personnel or operations.
- Trash. An activity known as "dumpster diving": the process of searching trash to gather data on people and activities.
- Open Source. Using published material that describes how we do things, who we are, and where we are located. Open source material can provide the criminal with an excellent profile of the agency.
- Human. The process of watching, listening, and asking questions about the abilities and intentions of the police department.

At one federal law enforcement agency, an assessment Of the OPSEC posture revealed that a comprehensive listing of all agents (including those under cover) with unit assignments was prepared on a monthly basis. When new listings were published, the old list was put in the wastebasket. On a regular basis, the trash was placed in clear plastic bags and left outside the building by the non-agency char force, where it was accessible to anyone passing by.

The adversary, using human intelligence methods (watching the normal operation), could have observed an opportunity to retrieve the trash bags, and may have gathered valuable information on the law enforcement operation. Once the problem was brought to the attention of management, the leaders directed that critical law enforcement information be marked "LEA Sensitive," ensuring that it would be disposed of in a secure manner.

Vulnerability Analysis

During this step, OPSEC addresses the capability of the adversary to use the information that has been collected in an attempt to block a police operation. This appraisal permits the planner to review the organization's activities to determine if the group is projecting intentions of its plans and whether or not the adversary has time to use this information.

The first phase of the analysis is to be attentive to the indicators associated with the mission. In OPSEC, indicators can be defined as any observable and/or detectable activities pointing to the critical information. Indicators may appear as innocent routine events, but often reflect patterns of predictable actions. They are the things police normally do in connection with their jobs—the things that seem very natural, but when compared to other activities done on a day-to-day basis will point to who we are, what we do, and how we do it.

For example, just prior to a raid, one agency had a practice of suiting-up in the parking lot adjacent to their office. The ritual included putting on an armored vest, racking a round into the shotgun, and other activities associated with that type of mission. When compared to other activities normally observed at the work site, the preparation for the raid served as an indicator of the intentions of law enforcement, particularly if the adversary was watching and waiting.

In another example, individuals working for an agency involved in undercover operations were issued four-door solid color sedans to perform their duties. The windows of these vehicles were tinted to provide protection for the undercover personnel from being identified by criminals. But the area where these officials worked prohibited tinting of vehicle windows. A person involved in a criminal venture, living in that area, might be suspicious if he happened to observe a vehicle fitting the above description parked down the street from his residence.

One officer related a situation he and his colleagues face with their department. Although undercover officers are assigned confiscated vehicles to perform their duties, the detectives must fuel their vehicles from the department's gas pump. All an adversary has to do is occasionally drive by the department and see if there are any non-traditional police vehicles being refueled. He can then document the description of the vehicles for future use.

During a recent hostage negotiation seminar, a person convicted of a crime spoke of his life in a right-wing extremism hate group. He related that prior to a combined federal and state police raid on the group's compound, the cult knew of the investigation and raid. They had spotted the police vehicles nine miles away. He stated the cars were new four-door standard police vehicles and that no one living in that geographic area could afford a new car. The cult also monitored police radio channels and frequently visited motels in the area where they looked for, out-of-state license plates on the vehicles, which they had identified as vehicles belonging to law enforcement.

The second part of this phase is to determine if the indicators are vulnerable to adversary exploitation. That is, are the clues associated with an operation available and susceptible to adversary exploitation? Does the criminal have sufficient time to take the information gathered from observing the indicators and counter the plans by changing his (the criminal's) behavior?

During this step, the manager would review the activities generally associated with the operation, determine if there are indicators pointing to the intention(s) of the police, and decide whether or not an adversary would have time to act on the information and block the mission if the indicators were observed by him. If there appeared to be a high degree of probability that these actions were vulnerable to exploitation, then a risk assessment would be conducted to determine if countermeasures were needed.

Countermeasures

The previous step addressed those indicators that reflect a high degree of vulnerability and have the potential of being exploited by the criminal. At this juncture, the case manager must decide whether possible loss of critical information through adversary exploitation justifies implementing countermeasures.

Questions concerning the chance of compromise and the consequences of such a compromise need immediate attention. During the examination, the cost of fixing the indicator must be weighed against the value of the information.

Once the indicators possessing a high degree of risk have been identified, the next step is the application of countermeasures. The word countermeasure refers to anything that effectively negates an adversary's ability to exploit vulnerabilities. The most effective countermeasures are simple, straightforward procedural adjustments that eliminate or minimize the generation of indicators.

Following a cost-benefit analysis, countermeasures should be implemented in priority order to protect those vulnerabilities having the most impact on the organization's mission. Countermeasures may include procedural changes, deception, perception management, speed of execution, stopping the mission, and other actions that protect the vital information.

Not for Law Enforcement Only

Although the intent of OPSEC is to ensure that information vital to a police operation is protected and the element of surprise is maintained, the process, whether intended or not, can be used by the criminal. An example of this came to light in an article published in a Washington, D.C., newspaper that reported drug dealers were lowering their profile. The article said that drug dealers, in an effort to camouflage themselves, were driving nondescript cars and wearing sweat suits and jeans to avoid detection by the police. The criminals realized that flashy cars, expensive clothes, and gold jewelry were indicators that assisted the police to identify that they were drug dealers. Recognizing that their vulnerability was high, the dealers applied the above-mentioned countermeasures to avoid being arrested.

We need to remember the OPSEC Golden Rule: What we do unto others can be done to us.

Operations Security can benefit various functions in law enforcement. Whether the activity is located in patrols, criminal investigations, special operations, or undercover operations, OPSEC can be a definite aid, providing greater security/protection for operations and personnel, and saving scarce resources.

Image that the patrol division of a medium-sized police department is working with the state police to transport a confidential informant for trial testimony due to a change in venue. Using the OPSEC process in planning the movement of the informant begins with the identification of critical information. Looking at it from the adversary's perspective, it might be determined that the vital data would include the following: date and time of movement, identity of the informant, method of transportation, route to be taken, resources to be employed (numbers and types of vehicles and personnel), time of arrival at the courthouse, and location of the safe house where subject may be located.

After identifying the information that needs protection, the next step would be to determine who the adversaries might be and their possible methods of collecting information. For this particular mission, the adversaries are identified as the accused, criminal associates, and the criminal (passive) network, including family members, sympathizers, and individuals paid to provide information to the criminals.

Methods of collecting information in this instance may include the following:

1. Communications—use scanners to monitor police radio networks and cellular phones.
2. Trash—retrieve discarded items, such as reports, manpower, and vehicle schedules, etc.
3. Open source—read newspapers and listen to commercial radio and TV to learn bits and pieces of vital information.
4. Human—use the total criminal network to watch, overhear, and follow the activities of patrol members associated with the operation.

The vulnerability analysis would consist of identifying predictable patterns of behavior that would project the intentions of the patrol division in their assigned task of transporting the informant. Some of the following indicators may exist:

1. Maintenance/preparation of the prisoner transport vehicles(s).
2. Unusual meetings (either in numbers or locations) between the patrol division, SWAT, the state police, and other agencies.
3. Communication about the plans over police radios.
4. Change in work patterns (working later).
5. Increased contact with court representatives.

If these (or similar) indicators were observed/detected by the adversary, and our plans projected, the vulnerability for exploitation would be high. If this were the case, then the risk would also be high, since the adversary would have sufficient time to act against the intentions of the police. This appraisal would determine whether or not countermeasures should be implemented.

Countermeasures appropriate for this mission might include the following:

1. Prohibiting the discussion of the operation over police radios.
2. Holding meetings between state police in neutral locations.
3. Making face-to-face contacts with court representatives.
4. Minimizing any change in work schedule/habits.
5. Ensuring that the public relations office is aware of the necessity of maintaining confidentiality of the operation.

Operations Security has proven its worth to the U.S. military, as well as to federal law enforcement. The benefit of retaining the element of surprise and protecting the integrity of the mission can provide the same valuable impact to state and local law enforcement. Not only will it increase the level of operational effectiveness, but, when used regularly, will enable the manager to view the operation from a unique perspective.

The viewpoint: Although there may be similarities, in each case there is a different set of circumstances that is based on a variety of elements that need to be viewed from the adversary's perspective. OPSEC allows the user to systematically look at each case in the specificity the mission requires and to adjust actions to meet the demands of the case.

What's Wrong with this Picture?

A member of a multi-agency counter drug task force was listening to the news as he drove to work. He was heading toward a rendezvous with other task force members to prepare for a pre-dawn raid on a public housing complex. The raid was to be a culmination of some eight months of tedious, painstaking investigative and administrative work by over 200 officers and agents. Now it was all for naught. The radio station was broadcasting the fact that an "impending enforcement action" was to take place in the housing complex that very morning. Needless to say, the raid was canceled. One of the agents in charge remarked: "If they know we're coming, we're not going."

How did this case take such an unfavorable twist? It was a situation of public relations gone awry. The city's PR machine, eager to inform its citizens about the active measures being taken to reduce the drug problem, released data the previous evening concerning the time and location of the upcoming raid. The story was picked up by local news organizations some 12 hours before the raid and was broadcast on an all-news station during the early morning hours.

Looking at this episode from the OPSEC process viewpoint, several steps can be easily discerned. A short quiz will illustrate the simplicity of the process.

1. What are the elements of critical information present?
   a) Fact that an enforcement action was to take place
   b) Date and time of the raid
   c) Location of the raid
   d) All of the above
2. Who might the adversary be?
   a) The PR office
   b) The media (newspaper, radio)
   c) The drug dealers
   d) The official who provided the data to the PR office
   e) All of the above
3. What is the threat or method of collection?
   a) Communications (in this case, public radio)
   b) Surveillance of task force members
   c) Both of the above
4. What level of vulnerability is there in this case?
   a) High
   b) Low
5. What are the risks (consequences of compromise) in the case?
   a) Waste of time and effort
   b) Injury or loss of life to law enforcement personnel
   c) Both of the above

6. What are some of the countermeasures we could use to avoid such a fiasco in the future?
   a) Tell fewer people about the raid
   b) Tell a small group of people directly related to the operation
   c) Only give out some minor points
   d) Use OPSEC during the planning stages of the operation
   e) All of the above

Answers to quiz: 1-d, 2-e, 3-c, 4~a*, 5-c, and 6-d

(* The vulnerability displayed in this situation is that the adversary is able to react to the news reports of the upcoming raid and move out of the area, and thus avoid arrest.)